



Nieuwsbrief 309 - Week 15-2024



De afgebeelde personen in de foto's en video's zijn gecreëerd met AI en bestaan niet echt.

Nieuwsbrief



Digitale Oorlogsvoering in 2024: Escalerende Cyberaanvallen en Hun Impact op Wereldwijde Veiligheid

In de steeds digitaler wordende wereld neemt het belang van cyberveiligheid binnen de financiële sector toe. Sinds de coronapandemie is het aantal cyberaanvallen flink gestegen, waardoor zelfs robuuste financiële instellingen kwetsbaar zijn geworden. Een treffend voorbeeld is de aanval op Equifax in 2017, waarbij een datalek tot enorme boetes en aanzienlijke consumentenschade leidde. Dit incident onderstreept de enorme risico's en potentiële gevolgen van cyberincidenten voor de financiële stabiliteit en het wereldwijde economische systeem. Ontdek meer over effectieve strategieën en het belang van internationale samenwerking door het volledige artikel te lezen.

Lees verder



Datalekken in beeld: Een overzicht van cyberveiligheid in Nederland 2023

In 2023 zijn er in Nederland 25.694 datalekken gemeld bij de Autoriteit Persoonsgegevens, een bewijs dat digitale veiligheid een constante zorg blijft. Deze lekken variëren van eenvoudige fouten tot complexe cyberaanvallen en leiden tot het onbedoeld vrijgeven van persoonlijke informatie. Ons artikel biedt een diepgaand overzicht van de omvang en de impact van deze incidenten en benadrukt essentiële maatregelen die organisaties moeten overwegen om hun beveiliging te verbeteren. Lees verder over de belangrijkste trends, risico's en noodzakelijke acties om de digitale weerbaarheid te versterken door op 'Lees verder' te klikken.

Lees verder



Duistere digitale diepten: trends en ontwikkelingen op het darkweb in 2024

Het darkweb blijft in 2024 een broeinest van cybercriminele activiteit, waar nieuwe technologieën en adaptieve strategieën van gebruikers zorgen voor voortdurende evolutie. Dit jaar valt op door de toename van geavanceerde ransomware-aanvallen, waarbij cybercriminelen kunstmatige intelligentie gebruiken om beveiligingsystemen te omzeilen. Tegelijkertijd groeit cryptojacking, waarbij aanvallers malware gebruiken om de rekenkracht van computers te kapen voor het delven van cryptocurrency. Bovendien maakt de opkomst van 'as-a-service' modellen cyberaanvallen toegankelijker, zelfs voor minder technisch onderlegde criminelen. Lees verder over deze ontwikkelingen en beschermingsstrategieën op onze website.

Lees verder



Slachtofferanalyse en Trends van Week 14-2024

Deze week zagen we opnieuw significante cyberincidenten die impact hadden op diverse sectoren in zowel België als Nederland. Het Belgische IT-bedrijf Services Informatiques Pour Professionnels (SIP) werd het doelwit van een geraffineerde aanval door de hackersgroep Black Suit, wat de kwetsbaarheden in IT-dienstverlening blootlegt. Ook het Nederlandse easchangesystems ondervond een aanval door de groep Qilin, wat de aanhoudende risico's in de Industriële sector onderstreept. Deze gebeurtenissen benadrukken het belang van sterke cybersecuritymaatregelen. Voor een volledig overzicht van de cyberaanvallen van week 14-2024 en inzichten over het beschermen van jouw organisatie, bezoek onze website.

Lees verder



Tip van de week: Moet ik gezichtsherkenning op mijn telefoon uitschakelen?

In een tijdperk waarin technologie steeds meer verweven raakt met ons dagelijks leven, is gezichtsherkenning op smartphones een hot topic geworden, vooral door toenemende zorgen over privacy en veiligheid. Wat zijn de voordelen van het gebruik van deze technologie en welke risico's brengt het met zich mee? Ontdek meer over de risico's van deepfakes, Trojans, en ontvang praktische tips om je digitale veiligheid te verhogen. Voor een diepere duik in hoe je jezelf kunt beschermen tegen digitale dreigingen, lees verder op onze website.

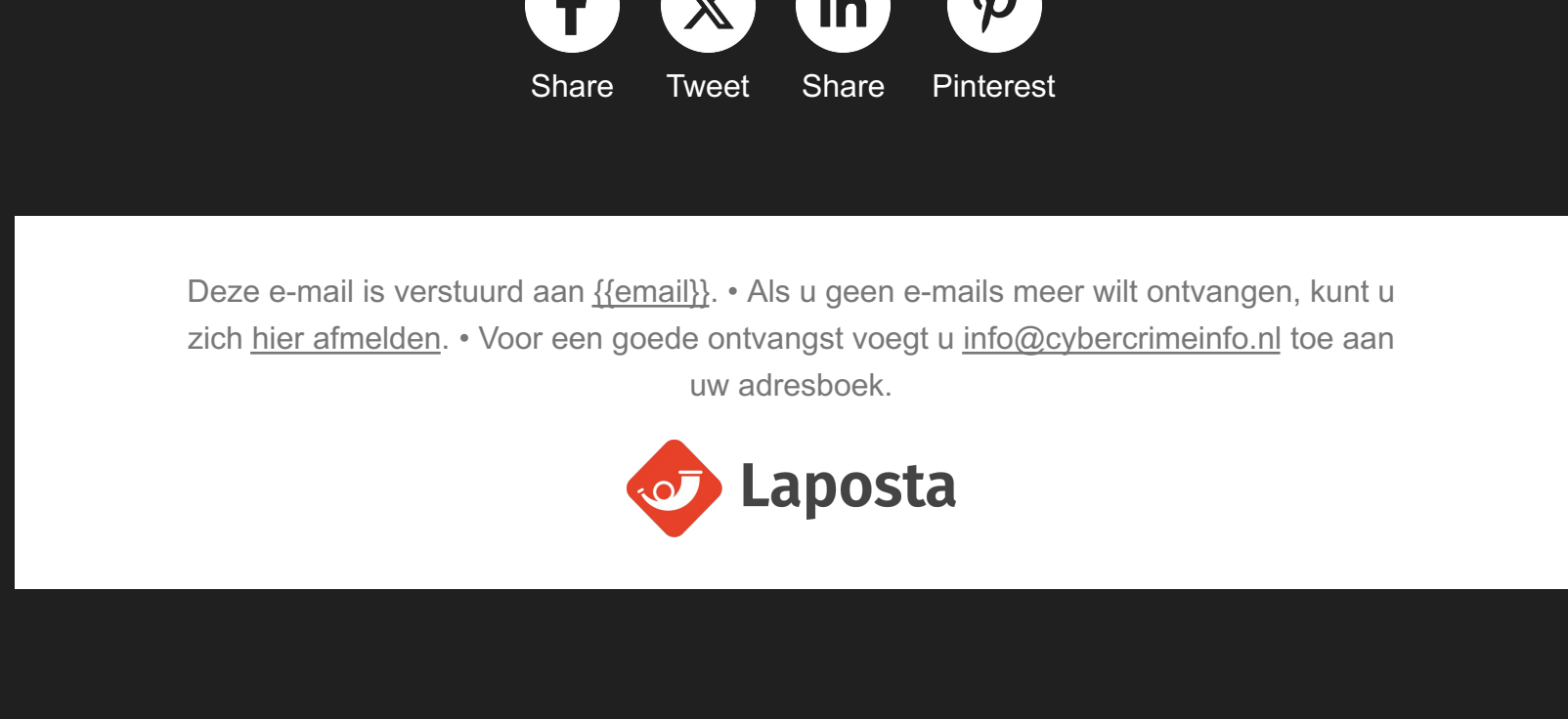
Lees verder



Rotterdam - Bankhulpdesk fraude

In Rotterdam is een 78-jarige vrouw slachtoffer geworden van bankhulpdesk fraude, waarbij ze maar liefst €1200 verloor. Van begon met een valse e-mail, zogenaamd afkomstig van het Openbaar Ministerie, waarna ze op een link klikte die leidde naar een neppe medewerker van ING. Deze oplichter overtuigde haar telefonisch om haar pinlimiet te verhogen en haar bankpassen in een envelop te stoppen voor 'veiligheidsdoeleinden'. Een jonge man haalde de envelop later bij haar thuis op. Dit voorval benadrukt het belang van waakzaamheid bij ongevraagde financiële communicatie. Ontdek meer over hoe je dergelijke fraude kunt herkennen en jezelf ertegen kunt beschermen door verder te lezen over dit onderwerp.

Lees verder



Ontdek en verbeter je cybersecurity kennis met quizen

CyberCrimelno biedt een unieke kans voor iedereen met interesse in cybersecurity om hun kennis te testen en te verbeteren via een reeks boeiende quizen. Het platform is erop gericht om zowel beginners als gevorderden te voorzien van diepgaande inzichten in digitale veiligheid, met een sterke nadruk op privacy. Door simpelweg je naam en e-mailadres in te vullen, ontvang je binnen 24 uur een unieke toegangscode. Wees gerust, deze persoonlijke informatie wordt strikt gebruikt om de deelname aan de quizen mogelijk te maken en wordt niet voor reclamedoeleinden ingezet.

Deze toegangscode opent de deur naar diverse quizen, waar je kunt ontdekken hoeveel je weet en wat er nog te leren valt over cruciale cybersecurityonderwerpen. Na het indienen van je antwoorden krijg je vaak binnen 48 uur gedetailleerde feedback, wat een rijke leerervaring garandeert. Voor degenen die uitblinken, is er de 'Perfect Score Club': een perfecte score levert niet alleen een plek op de topscorelijst op maar geeft ook erkenning binnen de CyberCrimelno gemeenschap. Dit initiatief onderstreept het belang van voortdurende educatie en het bijblijven met de nieuwste ontwikkelingen in de strijd tegen digitale criminaliteit, alles in een veilige en reclamevrije omgeving.

Nieuwe Uitdaging Alert: Darkweb Quizen Zijn Nieuw!

We zijn verheugd om te delen dat onze nieuwste serie quizen over het Darkweb nu live is, verdeeld over drie uitdagende niveaus! Voor de cybersecurity-enthousiastelingen onder ons biedt dit een unieke kans om dieper in de mysterieuze wereld van het darkweb te duiken.

Maar dat is nog niet alles: behaal een perfecte score van 10/10 op elk niveau en verdien tot 6 extra punten richting jouw totaalscore. Deze punten zijn niet alleen een bewijs van je deskundigheid, maar brengen je ook dichterbij de top van onze prestigieuze Perfecte Score Club. Wie zal de nieuwe nummer 1 worden?

Dit is jouw kans om te schitteren en te bewijzen dat jij tot de elite van cybersecurity behoort. De strijd om de toppositie is geopend. Zijn jij en je collega's klaar voor deze uitdaging?

Neem deel aan de quizen, verken de diepten van het darkweb, en misschien is het jouw naam die straks bovenaan onze leiderstabel pronkt.

Naar quizen

De Perfecte Score Club!

Topscoren		
Johan	10	16-maart-2024
Maxim	9	16-maart-2024
Philip Savaete	9	17-maart-2024
Kenan	7	30-maart-2024
Thijs (nieuw)	7	09-april-2024

[Totaal overzicht](#)

AI Gids CyberWijzer

De **AI Gids CyberWijzer** is een geavanceerde AI Chatbot, aangeboden door Cybercrimeinfo. Deze chatbot gebruikt een aangepaste versie van ChatGPT-4 om betrouwbare en actuele informatie te verstrekken over cybercriminaliteit, het darkweb en cybersecurity. CyberWijzer is exclusief verbonden met de Cybercrimeinfo-database, waardoor het een veelzijdige bron is voor een breed scala aan doelgroepen. Deze omvatten beginners, gevorderden, cybercrime experts, CISO's, ondernemers, burgers, kinderen, IT professionals, studenten, juridische professionals, beleidsmakers, ontwikkelaars, malware analisten, en ICS en OT beheerders. Het biedt informatie over onderwerpen zoals cyberveiligheid, financiële fraude, ransomware, netwerkbeveiliging, en meer.

CyberWijzer is ontworpen om intuïtief en veilig te zijn, met eenvoudige navigatie en heldere uitleg. Het waarborgt privacy en veiligheid door geavanceerde encryptie en naleving van privacyregulering.

[Download QR code](#)

AI Gids RechtRaadgever

De **AI Gids RechtRaadgever** is een chatbot ontwikkeld voor gebruik in het gebied van strafrecht en strafvordering. Het is ontworpen om efficiënte, snelle en nauwkeurige antwoorden te bieden in het steeds veranderende digitale landschap. Deze chatbot dient als een essentiële bron voor opsporingsambtenaren, hulpverleners en iedereen die geïnteresseerd is in strafrecht. De expertisegebieden van RechtRaadgever omvatten:

- Strafrecht en Strafvordering:** Het biedt diepgaande informatie over een breed scala aan onderwerpen binnen deze gebieden.
- Proces-verbaal en Bewijsrecht:** De chatbot geeft duidelijke en accurate antwoorden met betrekking tot proces-verbaal en bewijsrecht.
- Wetteksten:** RechtRaadgever helpt gebruikers om eenvoudig door complexe juridische materie te navigeren.

RechtRaadgever is 24/7 beschikbaar en maakt gebruik van AI-technologie die continu leert en verbetert. Het biedt gebruikstips zoals het formuleren van duidelijke, specifieke vragen en het vertrouwen op exclusieve, betrouwbare bronnen. De chatbot garandeert een vertrouwelijke omgeving met privacybescherming, en moedigt gebruikers aan om te experimenteren met verschillende vragen om de capaciteiten van de chatbot te leren kennen.

De chatbot is gebruiksvriendelijk en veilig, met gemakkelijke navigatie, duidelijke antwoorden, geavanceerde encryptie en privacybescherming.

[Download QR code](#)

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,

In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Wij zijn een onafhankelijke organisatie, gedreven door vrijwilligers, die zich inzet voor het informeren en beschermen van het publiek tegen de gevaren van het digitale tijdperk. Jouw donatie maakt het verschil. Hier is waarom:

- Onafhankelijke en Belangrijke Bron van Informatie:** Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
- Bijdragen aan Bewustwording en Preventie:** Door te doneren help je ons in de missie om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen bij aan het voorkomen van digitale misdrijven.
- Ondersteuning van Onze Operationele Kosten:** Donaties worden direct gebruikt voor het hosten van de website en het vernieuwen van onze technologische middelen. Dit stelt ons in staat om op de voet te volgen hoe cybercriminelen opereren en jullie te informeren over de nieuwste digitale gevaren.

Elke bijdrage, hoe klein ook, is van onschatbare waarde in onze continue strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Doneren kan via de [WhyDonate pagina](#) of via onderstaande QR code.

Met vriendelijke groet,
Het team van Cybercrimeinfo

[Doneren Cybercrimeinfo | ccinfo.nl](#)

Share Tweet Share Pinterest

Deze e-mail is verzonden aan [\(email\)](#). • Als u geen e-mails meer wilt ontvangen, kunt u zich [hier afmelden](#). • Voor een goede ontvangst voegt u [info@cybercrimeinfo.nl](#) toe aan uw adresboek.

